Haaga-Helia
ammattikorkeakoulu Oy

Windows päivitysten keskitetty hallinta WSUS –palvelun avulla

Henry Kujanpää

Opinnäytetyö
Tietojenkäsittelyn -
koulutusohjelma
2017

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Henry Kujanpää

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Windows päivitysten keskitetty hallinta WSUS –palvelun avulla

Sivu- ja liitesivumäärä
24

Tietoturva on jatkuvasti esillä niin mediassa ja työpaikoillakin. Kun tietokone yhdistetään verkkoon, on se saman tien alttiina useille tietoturvauhkille. Yksi tavoista ehkäistä haittaohjelmille alttiiksi joutumista on järjestelmien pitäminen ajan tasalla.

Windows päivitysten keskitetty hallinta WSUS –palvelun avulla opinnäytetyö käynnistettiin syksyllä 2017 tekijän halusta kehittää Windows -palvelin osaamistaan. Aihe valikoitui tekijän mielenkiinnosta tietoturvaa ja Windows –käyttöjärjestelmiä kohtaan. Työ oli toiminnallinen opinnäytetyö ja työllä ei ollut toimeksiantajaa. Motivaatio työhön löytyi tekijän halusta kehittää omaa ammatillista osaamistaan asennus ja konfigurointio toimenpiteitä hyödyntäen.

Työn tavoitteena oli luoda testiympäristö Haaga-Helian Ammattikorkeakoulun CloudPlatform virtuaaliympäristöön. Testiympäristöön asennettiin virtuaalipalvelin ja siihen otettiin käyttöön Windows Server Update Service –palvelu. Testiympäristöön asennettiin neljä virtuaalityöasemaa, joihin jaettiin Windows päivitykset keskitetysti WSUS-palvelun avulla. Työn tavoitteena oli antaa peruskäsitys WSUS-palvelun konfiguroinninsta, tietoturvauhkista, sekä kertoa tarkemmin eri tyyppisistä Windows -päivityksistä.

Työn alussa käsitellään erilaisia haittaohjelmia ja perehdytään siihen mitä haittaohjelmat ovat. Tämän jälkeen perehdytään Windows –päivityksiin ja niiden eri tyyppeihin. Projektin pääasiallinen tavoite oli tutkia WSUS-palvelun käyttöönottoa ja kertoa mikä WSUS-palvelu oikein on. Tavoiteltu lopputulos oli luoda testiympäristö mikä pitää sisällään WSUS-palvelimen, sekä työasemia, joille Windows –päivitykset jaetaan keskitetysti Windows Server Update –palvelun avulla.

Työn lopussa käsitellään projektin onnistumisia, epäonnistumisia, haasteita, sekä tekijän mietteitä Windows Server Update Service –palvelusta.

Asiasanat
Windows Server Update Services, Päivitykset, Tietoturva

Sisällys

1 Johdanto

Tietoturva on jatkuvasti esillä niin mediassa ja työpaikoillakin. Kun tietokone yhdistetään verkkoon, on se saman tien alttiina useille tietoturvauhkille. Yksi tavoista ehkäistä haittaohjelmille alttiiksi joutumista on järjestelmien pitäminen ajan tasalla.

Windows päivitysten keskitetty hallinta WSUS –palvelun avulla opinnäytetyö käynnistettiin syksyllä 2017 tekijän halusta kehittää Windows -palvelin osaamistaan. Aihe valikoitui tekijän mielenkiinnosta tietoturvaa ja Windows –käyttöjärjestelmiä kohtaan. Työ oli toiminnallinen opinnäytetyö ja työllä ei ollut toimeksiantajaa. Motivaatio työhön löytyi tekijän halusta kehittää omaa ammatillista osaamistaan asennus ja konfigurointi toimenpiteitä hyödyntäen.

Työn tavoitteena oli luoda testiympäristö Haaga Helian Ammattikorkeakoulun CloudPlatform virtuaaliympäristöön. Testiympäristöön asennettiin virtuaalipalvelin ja siihen otettiin käyttöön Windows Server Update Service –palvelu. Testiympäristöön asennettiin neljä virtuaalityöasemaa, joihin jaettiin Windows päivitykset keskitetysti WSUS-palvelun avulla. Työn tavoitteena oli antaa peruskäsitys WSUS-palvelun konfiguroinninsta, tietoturvauhkista, sekä kertoa tarkemmin eri tyyppisistä Windows -päivityksistä.

Työn alussa käsitellään erilaisia haittaohjelmia ja perehdytään siihen mitä haittaohjelmat ovat. Tämän jälkeen perehdytään Windows –päivityksiin ja niiden eri tyyppeihin. Projektin pääasiallinen tavoite oli tutkia WSUS-palvelun käyttöönottoa ja kertoa mikä WSUS-palvelu oikein on. Tavoiteltu lopputulos on luoda testiympäristö mikä pitää sisällään WSUS-palvelimen, sekä työasemia joille Windows –päivitykset jaetaan keskitetysti Windows Server Update –palvelun avulla.

1.1 Käsitteet

Aktiivihakemisto (Active Directory)	Aktiivihakemisto on Windows palvelinten toimialueen tietokanta ja hakemisto, jonka avulla hallitaan käyttäjätunnuksia, ryhmiä, sekä tietokonetilejä.
CloudPlatform	Haaga Helian Ammattikorkeakoulun käyttämä pilvipalvelu, johon oppilaiden on mahdollista asentaa virtuaalipalvelimia ja -työasemia.
Metatieto (Metadata)	Metatieto on yhteenveto tiedoista. Metatieto helpottaa tietojen löytämistä ja työskentelyä tietolähteiden avulla.
Nimipalvelujärjestelmä (Domain Name System, DNS)	DNS on nimipalvelujärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi.
Instanssi (Instance)	Instanssi on pilviympäristössä toimiva virtuaalitietokone.
Käyttöjärjestelmä (Operating System)	Käyttöjärjestelmä on tietokoneen tarvitsema välttämätön ohjelmisto, joka toimii tietokoneen laitteiston ja muiden ohjelmistojen välissä tarjoten niille erilaisia palveluita.
Organisaatioyksikkö (Organization Unit, OU)	Organisaatioyksikkö on aktiivihakemiston säilö, joka voi pitää sisällään käyttäjiä, käyttäjäryhmiä ja tietokoneita. Organisaatioyksikön avulla voidaan määrittää ryhmäkäytäntöjä koskemaan vain tiettyjä käyttäjiä.
Palvelin (Server)	Palvelin on tietokone, joka tarjoaa palvelinohjelmistojen avulla erilaisia palveluja muille ohjelmille.
Rooli (Role)	Palvelimen roolilla tarkoitetaan Windows –palvelimissa Server Managerista asennettavia ohjelmistoja.
Ryhmäkäytäntö (Group Policy)	Ryhmäkäytännöillä hallitaan toimialueen käyttäjätunnuksien ja työasemien asetuksia.
Toimialue (Domain)	Toimialue on ryhmä verkossa olevia tietokoneita ja laitteita, joita hallitaan keskitetysti järjestelmänvalvojien toimesta.
Upstream -palvelin	Upstream -palvelimella tarkoitetaan palvelinta, joka tarjoaa jotakin tiettyä palvelua toiselle palvelimelle.

2 Haittaohjelmat

Malware eli haittaohjelma lyhenne tulee sanoista ”malicious software”. Haittaohjelma on ohjelma, joka on tietoisesti ohjelmoitu aiheuttamaan vahinkoa tiedostoille, laitteille tai ihmisille. Kun puhutaan viruksista, troijalaisista tai vakoiluohjelmista tarkoitetaan niillä haittaohjelmien eri tyyppejä. (Jonathan Lemonnier 2015)

2.1 Virus ja mato (worm)

Virukset ja madot ovat parhaiten tunnetut haittohjelmien tyypit. Ne ovatkin saaneet nimensä niiden tavasta levitä järjestelmässä. (Andrew Bettany, Mike Halsey 2017, 4). Virus kiinnittää itsensä puhtaisiin tiedostoihin ja leviää tartuttamalla myös muut puhtaat tiedostot. Virus voi levitä hallitsemattomasti vahingoittaen järjestelmän ydintoimintoja, sekä poistaa tai vioittaa tiedostoja. Useimmiten virukset leviävät suoritettavien tiedostojen kautta. Madot taas tartuttavat koko verkon laitteita, joko paikallisesti tai ulkoisesti käyttämällä verkkoyhteyksiä. Madot käyttävät hyödykseen jokaista tartunnan saanutta laitetta levitäkseen muihin laitteisiin. (Jonathan Lemonnier 2015).

Viruksen tartuttama tietokone saattaa olla hidas, aiheuttaa selittämättömiä levy ja verkko tapahtumia, tiedostot eivät aukea oletusohjelmilla, sekä ponnahdusikkunoita tai taustakuvia ilmestyy tietokoneelle. (Andrew Bettany, Mike Halsey 2017, 41)

2.2 Vakoiluohjelma (Spyware)

Vakoiluohjelma on suunniteltu käyttäjän vakoiluun. Vakoiluohjelma kerää tietoa mitä tietokoneella tehdään verkossa. Esimerkiksi se kerää salasanoja, luottokortin numeroita, sekä käyttäjän internetin selaushistoriaa. (Jonathan Lemonnier 2015)

2.3 Mainosohjelma (Adware)

Mainosohjelma on haittaohjelmista ehkäpä vaarattomin. Mainosohjelman tarkoitus on esittää mainoksia käyttäjän tietokoneella. Mainokset ilmenevät usein ponnahdusikkunoina selaimessa tai erillisenä ohjelmana. Mainosohjelma itsessään ei ole todellinen uhka, ellei mainosohjelman mukana asennu haittaohjelmia, kuten esimerkiksi näippäilyn tallentaja (keylogger). (Andrew Bettany, Mike Halsey 2017, 4)

2.4 Troijalaiset (Trojan)

Troijalainen esiintyy yleensä käyttäjälle vaarattomana hyödyllisenä ohjelmana, mutta pitää todellisuudessa sisällään haavoittuvuuden järjestelmään. Se pyrkii luomaan takaoven (backdoor) tietoturvaan ja päästämään muita haittaohjelmia sisään tietokoneeseen. (Jonathan Lemonnier 2015). Takaovi tekniikan avulla hakkeri pääsee luvattomasti käsiksi tietokoneeseen verkon välityksellä.

2.5 Kiristysohjelma (Ransomware)

Kiristysohjelma voi esimerkiksi lukita tietokoneen ja uhata työaseman tiedostojen tyhjentämistä tai tuhoamista, mikäli hakkerille ei makseta tiettyä summa rahaa. (Jonathan Lemonnier 2015)

3 Windows päivitykset

Windows update on Windows käyttöjärjestelmien sovellus, joka pitää käyttöjärjestelmän ajan tasalla Microsoft tuotteiden tietoturvaan, vakauteen ja toimintoihin liittyvillä päivityksillä. Windows update -sovellusta ei suositella otettavan pois käytöstä muissa kuin erikoistapauksissa, sillä päivittämätön käyttöjärjestelmä altistaa tietokoneen tietoturvauhkille. (Andrew Bettany, Mike Halsey 2017, 13). Windows update -ominaisuus on ollut käytössä Windows -työasemissa Windows 98 -käyttöjärjestelmän julkaisusta lähtien.

3.1 Windowsin automaattiset päivitykset

Windows järjestelmissä on mahdollista asentaa Windowsin päivitykset automaattisesti työasemalle Windowsin automaattiset päivitykset -toiminnon avulla. Käyttämällä automaattiset päivitykset -ominaisuutta Windows päivityksiä ei tarvitse hakea erikseen Microsoft Update -sivuston kautta, vaan Windows havaitsee päivitykset automaattisesti ja lataa ne tietokoneelle. Automaattiset päivitykset -ominaisuus tunnistaa, että työasema on verkossa ja hakee päivitykset automaattisesti Windows Update -sivustolta. Käyttäjän työasemalle ilmestyy kuvake joka ilmoittaa, että uusia päivityksiä on saatavilla. (MicrosoftSupportB). Tämä ominaisuus on kätevä esimerkiksi kotikoneissa, mutta yritysmaailmassa ominaisuuden käyttöönottoa kannattanee harkita. Mikäli Windows -päivitykset asentuvat automaattisesti ja hallitsemattomasti työasemille yritysympäristössä on työasemien ylläpitäminen ja valvonta järjestelmänvalvojille huomattavasti haastavampaa. Windows Server Update Service onkin yksi tavoista korvata Windowsin automaattiset päivitykset.

3.2 Windows päivitysten tyypit

Kriittinen päivitys (Critical update) – on päivitys joka korjaa tietyn tietoturvaan liittymättömän kriittisen ohjemointivirheen. Kyseinen ohjelmointivirhe voi aiheuttaa esimerkiksi vakavan toimintahäiriön tai häiritä sovellusten yhteensopivuutta. (Rafal Sosnowski 2016)

Määritelmä päivitys (Definition update) – on laajasti julkaistu säännöllinen ohjelmistopäivitys, joka pitää sisällään määritelmä tietokannan lisäosia. Määritelmä tietokantoja käytetään yleensä havaitsemaan tiettyjä attribuutteja, kuten haittaohjelmien koodia, tietojen kalastelu sivustoja tai roskapostia. (Microsoft SupportA)

Tietoturvapäivitys (Security update) – on päivitys joka korjaa tietoturva haavoittuvuuksia. Tietoturvapäivityksillä on viisi kriittisyys tasoa, jotka Microsoft Security Response Center määrittelee. (Rafal Sosnowski 2016)

Huoltopäivitys (Service Pack) – on päivitys, joka usein yhdistää aiemmin julkaistut päivitykset. Päivitys voi pitää sisällään tietoturva korjauksia, parannuksia suorituskykyyn, sekä tuen uusille laitteistoille. (Microsoft SupportA)

Hotfix – on ohjelmistopäivitys, joka on suunniteltu korjaamaan bugi tai tietoturva-aukko ohjelmassa. Hotfixejä kehitetään kriittisesti ja julkaistaan mahdollisimman nopeasti ohjelmistovirheiden välttämiseksi. (TechTarget 2015)

Update rollup – on testattu päivityspaketti, joka pitää sisällään huoltopäivityksiä, tietoturvapäivityksiä, kriittisiä päivityksiä ja päivityksiä, jotka on pakattu yhteen helpon jaeltavuuden vuoksi. Rollup on yleensä kohdistettu tietylle osa-alueelle, kuten tietoturva tai tuotteen komponentit esimerkiksi Internet Information Services (IIS). (Microsoft SupportC)

Päivitys (Update) – on päivitys joka ei ole kriittinen ja korjaa yleensä ohjelmointivirheen, johon ei liity tietoturvauhkaa. (Microsoft SupportC)

Feature Pack – on uusi tuoteominaisuus, joka jaetaan ensimmäisen kerran tuotteen julkaisun ulkopuolella ja se tulee tyypillisesti seuraavan tuotejulkaisun mukana. (Microsoft SupportC)

Ajuri (Driver) – on ohjelmisto, jolla hallitaan sisääntulevia ja ulostulevia laitteita. (Microsoft SupportC)

Tool – Apuohjelma tai ominaisuus, joka mahdollistaa tehtävän tai tehtävien suorittamisen. (Microsoft SupportC)

3.3 Microsoft Security Response Center

Microsoft Security Response Center (MSRC) on vuodesta 2002 lähtien toiminut Microsoftin työryhmä, joka on sitoutunut tarjoamaan suojatumman, yksityisen, sekä luotettavamman tietojenkäsittely kokemuksen. MSRC valvoo ja käsittelee tietoturvauhkia, sekä vastaanottaa asiakkaiden havaitsemia tietoturva epäilyjä. Microsoft tuotteiden tietoturvauhkien epäilyksiä varten on oma sähköpostiosoite: secure@microsoft.com. MSRC käsittelee vuodessa n. 150,000 sähköpostia liittyen Microsoft tuotteiden tietoturvauhkiin. (TechnetA)

Microsoft Security Response Centerin kriittisyystasot ovat:

Critical (Kriittinen) – Päivitys korjaa haavoittuvuuden joka saattaa mahdollistaa internet madon leviämisen ilman käyttäjän tekemiä toimenpiteitä.

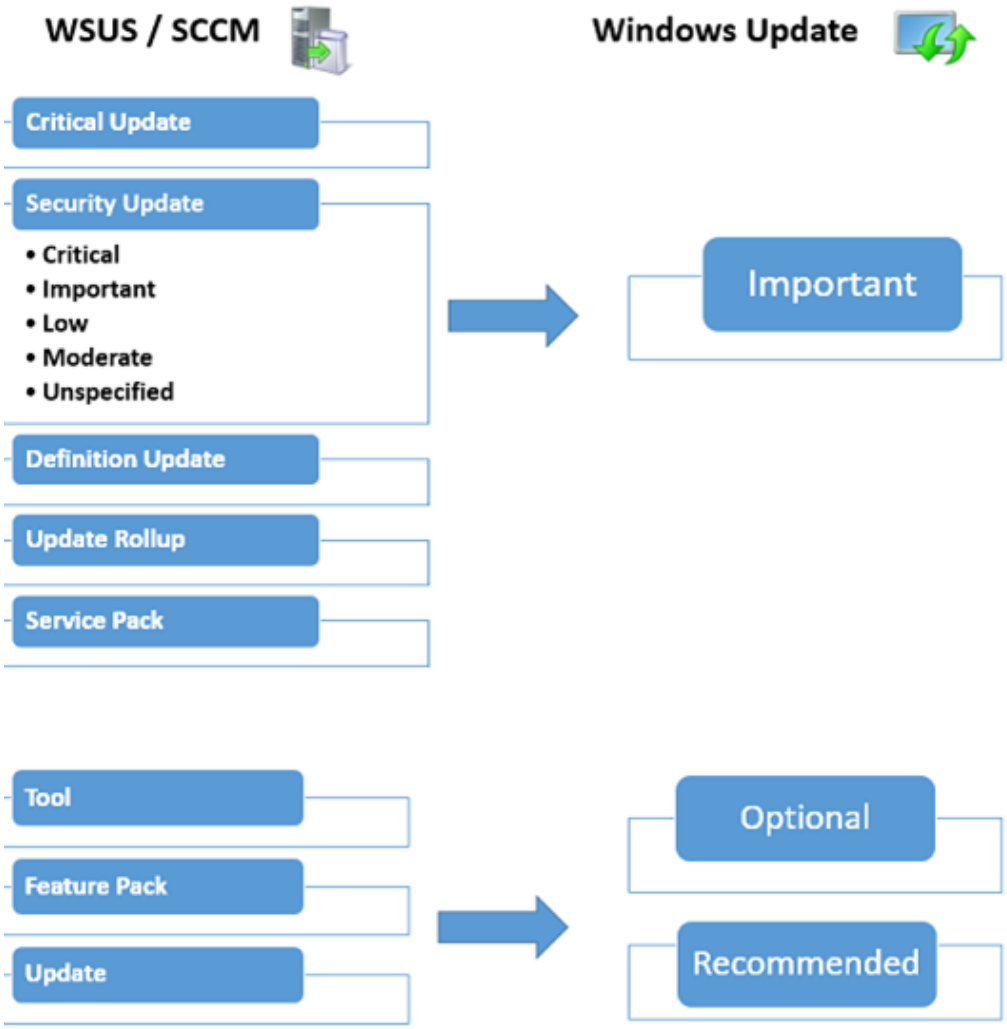
Important (Tärkeä) – Päivitys korjaa haavoittuvuuden, joka on uhka käyttäjän tietojen luotettavuudelle, eheydelle, tai käytettävyydelle.

Low (Matala) – Päivitys korjaa haavoittuvuuden jonka hyödyntäminen on äärimmäisen vaikeaa tai jonka vaikutus on vähäinen.

Moderate – Päivitys korjaa haavoittuvuuden jonka vaikutuksia voidaan vähentää todentamisvaatimuksilla tai kofiguroinnilla.

Unspecified – Päivityksellä ei ole kriittisyys astetta. (Rafal Sosnowski 2016)

Rafal Sosnowski on kuvannut hyvin alla olevassa kuvassa, kuinka Windows päivitykset näkyvät WSUS ja SCCM -ohjelmistoissa ja kuinka ne esiintyvät Windows Update -ohjelmassa käyttäjän tietokoneella. Kriittiset päivitykset, tietoturvapäivitykset, määritelmäpäivitykset, update rollupit ja huoltopäivitykset näkyvät Windows update -ohjelmistossa tärkeinä päivityksinä. Tool, Feature pack ja päivitys näkyvät valinnaisina tai suositeltuina päivityksinä.



Kuva 1. Windows Update kategoriat (Rafal Sosnowski 2016, hakupäivä 13.10.2017)

4 Mikä on WSUS?

Windows Server Update Services (WSUS) tunnetaan myös nimellä Software Update Services (Update) on Windows –palvelinten mukana tuleva rooli, jonka käyttöönotto, konfigurointi, sekä poistaminen on mahdollista Windows -palvelimen Server Managerin avulla.

Windows Server Update Services (WSUS) mahdollistaa viimeisimpien Microsoft ohjelmistojen päivitysten jakamisen keskitetysti tietokoneisiin ja palvelimiin. WSUS-palvelun avulla pystytään jakamaan Microsoftin päivityksiä samassa toimialueessa oleviin tietokoneisiin. Päivitysten jakaminen tapahtuu WSUS –palvelimelta WSUS -hallintakonsolista. WSUS –palvelin voi myös toimia päivitysten lähteenä muille palvelimille organisaation sisällä. WSUS –palvelinta joka toimii päivitysten lähteenä, kutsutaan upstream -palvelimeksi. Mikäli WSUS-palvelimia on useampi organisaation sisällä, vähintään yhden WSUS –palvelimen on oltava yhdistettynä Microsoft Update –palveluun. Järjestelmävalvoja määrittää verkon tietoturvan ja konfiguroinnin mukaisesti, kuinka moni muu WSUS –palvelin on yhdistettynä suoraan Microsoft Update-palveluun. (Corey Plett, Liza Poggemeyer 2017)

4.1 Kuinka WSUS toimii?

Oletuksena WSUS-käyttää HTTP -protokollan porttia 80 ja HTTPS -protokollan porttia 443 päivitysten lataamiseksi Microsoftilta. WSUS vaatii toimiakseen tietokannan jokaiselle WSUS-palvelimelle. WSUS tietokanta pitää sisällään WSUS -palvelimen konfigurointi tiedot, sekä metatietoa joka kuvaa jokaista päivitystä, tietoa asiakastietokoneista, päivityksistä ja vuorovaikutuksesta. (Corey Plett, Liza Poggemeyer 2017)
Ensimmäisen kerran kun tietokone ottaa yhteyttä WSUS -palvelimeen, palvelin skannaa asiakastietokoneen selvittäen mitkä päivitykset tietokoneelle on jo asennettu ja mitä päivityksiä se vielä tarvitsee. Kun järjestelmänvalvoja hyväksyy päivityksen asiakastietokoneelle asennettavaksi, tietokone lataa päivityksen seuraavalla kerralla, kun tietokone on yhteyksissä WSUS-palvelimeen. (Utilize Windows 2010)

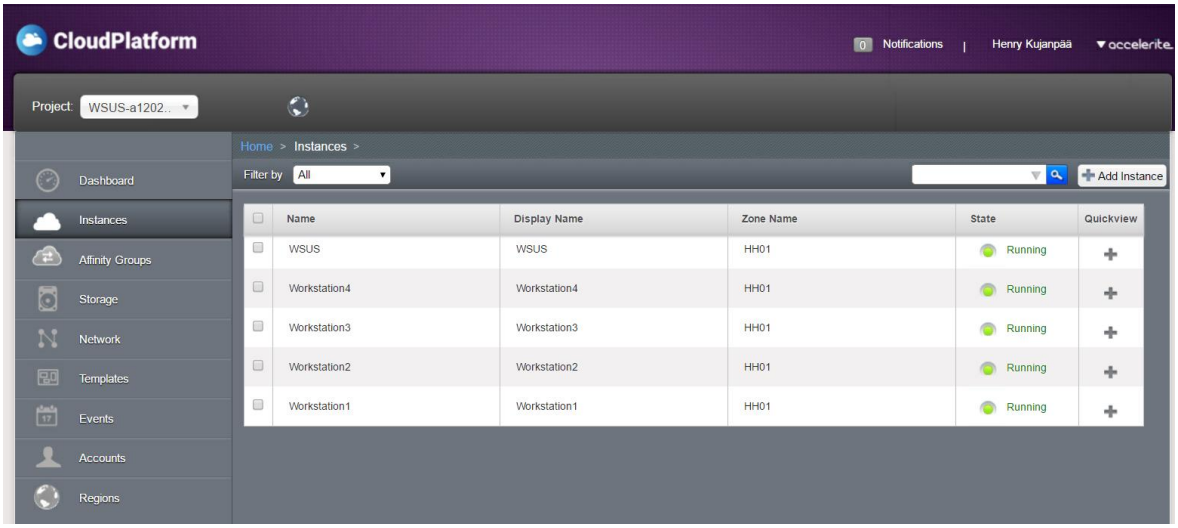
4.2 Päivitysten hallinta prosessina

Päivitysten hallinta on prosessi, jonka avulla hallitaan ohjelmistopäivitysten käyttöönottoa ja ylläpitoa tuotantoympäristöihin. Se auttaa ylläpitämään toiminnan tehokkuutta ja ratkaisemaan tietoturvahaavoittuvuuksia, sekä ylläpitämään tuotantoympäristön vakaana. Mikäli organisaatio ei pysty määrittämään ja ylläpitämään tiettyä luottamustasoa

käyttöjärjestelmissä ja sovelluksissa, saattaa siitä seurata useita tietoturvahaavoittuvuuksia, jotka saattavat johtaa salaisen tiedon vuotamiseen, sekä pääoman menettämiseen. Tämän uhkan minimoiminen edellyttää, että järjestelmät ovat konfiguroitu oikein, sekä uusimmat ohjelmistot ja suositellut ohjelmistopäivitykset ovat asennettu tuotantoympäristöön. Yrityksen pääasialliset hyödyt WSUS –palvelusta ovat: keskitetty päivitysten hallinta, sekä päivitys hallinnan automatisointi. (Corey Plett, Liza Poggemeyer 2017)

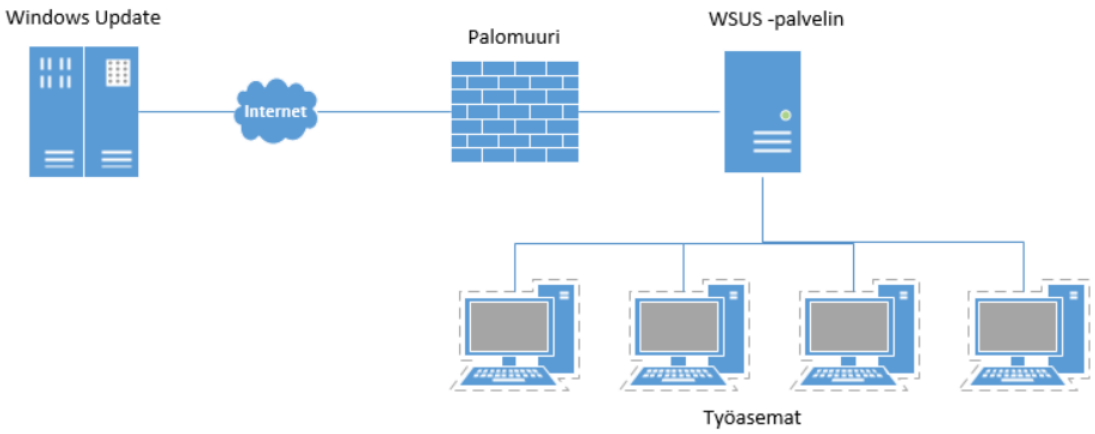
5 Projektiympäristö

Projektin käytännön osuus suoritettiin Haaga-Helian Ammattikorkeakoulun CloudPlatform pilviympäristössä. Loin CloudPlatform -pilvipalveluun viisi instanssia WSUS, Workstation1, Workstation2, Workstation3 ja Workstation4. WSUS -nimiseen instanssiin asennettiin 64-bittinen Windows Server 2012 R2. WSUS -virtuaalipalvelimelle asetettiin levytilaa 50Gt, muistia 2Gt ja prosessorina toimii kaksi ytiminen Intel Xeon CPU E5-2630 2.30GHz. Workstation1 ja Workastation4 -työasemille asennettiin 64-bittinen Windows 7 -käyttöjärjestelmä ja Workstation2 ja -3 työasemiin asennettiin 64-bittinen Windows 8.1 -käyttöjärjestelmä. Virtuaalityöasemille asetettiin levytilaa 20Gt, muistia 1 Gt ja prosessorina toimii kaksi ytiminen Intel Xeon CPU E5-2630 2.30GHz. Kuvassa 2. näkyy CloudPlatform virtuaaliympäristöön luodut instanssit.



Kuva 2. CloudPlatform virtuaaliympäristöön luotu testiympäristö.

CloudPlatformiin piti myös luoda oma verkko. Nimesin verkon nimellä: ”WSUS”. Verkko konfiguroitiin niin, että palvelimelta ja työasemilta on myös mahdollista päästä käsiksi julkiseen verkkoon. CloudPlatformista WSUS-verkkoon tuli myös avata portti 80, että etätyöpöytäyhteydet palvelimeen ja työasemiin onnistuivat Haaga-Helian ammattikorkeakoulun verkosta. Kuvassa 3. kuvataan projektiympäristö ja kuinka palvelin on yhteydessä Windows Update –palveluun ja työasemiin verkon avulla.



Kuva 3. Projektiympäristön toiminta.

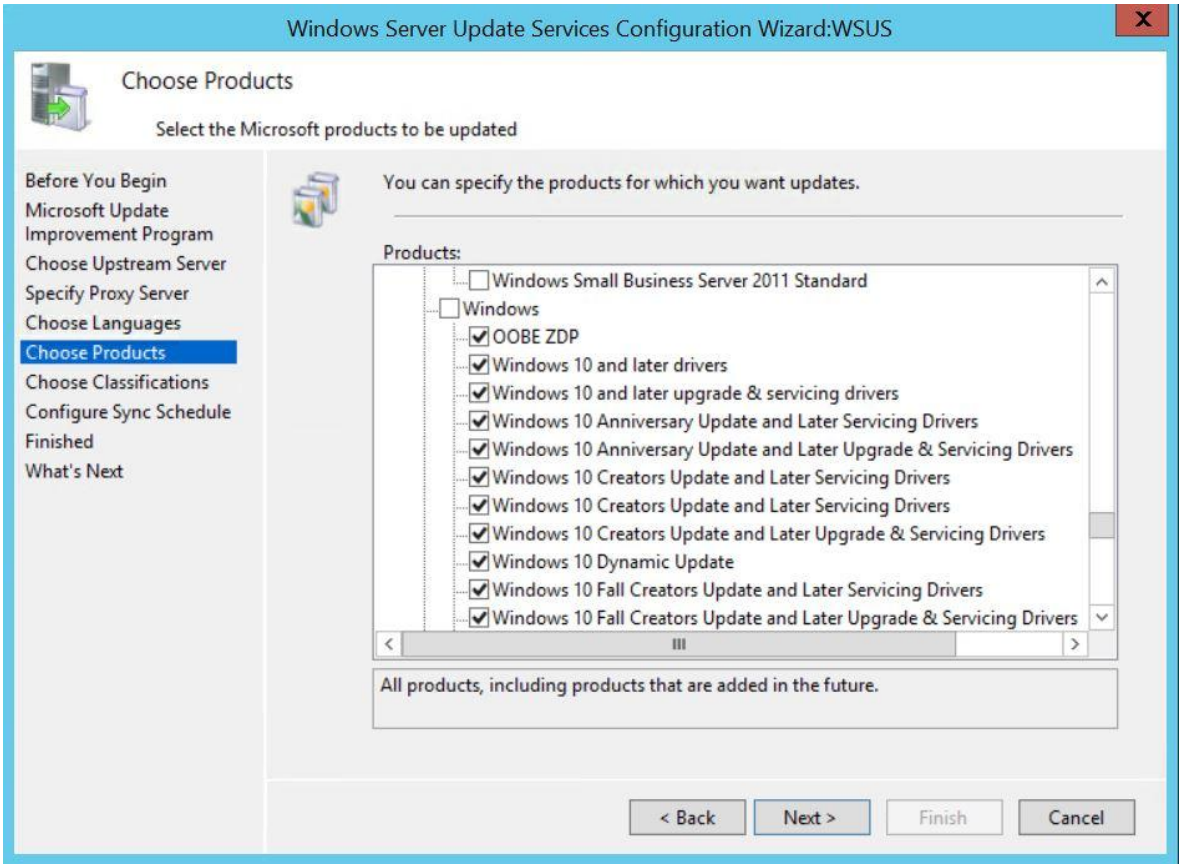
Projekti alkoi palvelimen ja työasemien asennuksella ja konfiguroinnilla. Palvelimelle luotiin metsä ja toimialue, sekä asennettiin Aktiivihakemisto ja DNS-palvelu. Palvelin käyttää IPv4 -protokollaa ja palvelimelle määritettiin kiinteä IP-osoite. IPv6 -protokolla otettiin kokonaan pois käytöstä, että mahdollisilta verkko-ongelmilta vältyttäisiin.

Työasemat liitettiin toimialueeseen ja niille asetettiin kiinteät IP-osoitteet. Myös työasemat käyttävät IPv4 -protokollaa ja IPv6 -protokolla otettiin kokonaan pois käytöstä.

5.1 WSUS -palvelun asennus ja konfigurointi

Ennen WSUS-roolin konfigurointia ja käyttöönottoa tulee varmistaa, että palvelimen laitteisto on riittävän tehokas ohjelmiston käyttöä varten. WSUS-roolin minimi laitevaatimukset ovat 1.4 Ghz prosessori, 2Gt muistia, 10Gt levytilaa, 100 MB/s verkkoadapteri. (Corey Plett, Liza Poggemeyer 2017).

Windows Server Update Services -rooli otettiin käyttöön WSUS -palvelimella Add Roles and Features Wizardista. Määritin WSUS-roolin tallentamaan päivitykset C-aseman juureen, kansioon WSUS_UPDATES. Valitsin päivitysten kieleksi ainoastaan Englannin, koska työasemissa on Englannin kieliset Windows -käyttöjärjestelmät. Valitsin Windows Server Update Services konfiguroinnissa ainoastaan käyttöjärjestelmien päivitykset, sillä työasemiin ei ole asennettu esimerkiksi Microsoft Office -tuotteita.



Kuva 4. Valitaan mille käyttöjärjestelmille tai ohjelmistoille päivityksiä haetaan.

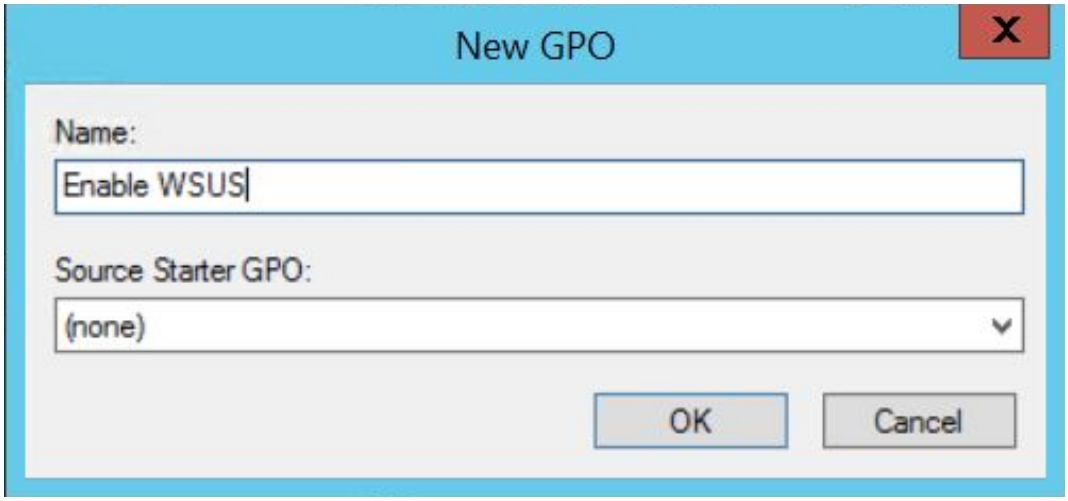
5.2 Ryhmäkäytäntöjen määrittäminen

Järjestelmänvalvojat konfiguroivat ja määrittävät ryhmäkäytäntöjä luomalla ryhmäkäytäntö objekteja. Ryhmäkäytäntö objektit ovat asetusten ryhmiä, joita voidaan kohdentaa koskemaan käyttäjä -, sekä tietokonetilejä aktiivihakemiston kautta. Ryhmäkäytäntö objekteja luodaan Group Policy Management Editorin avulla. Ryhmäkäytäntöjen avulla voidaan esimerkiksi laittaa jokin tietty ohjemisto asentumaan kaikkien käyttäjien työpöydille. Ryhmäkäytäntö objekteja on kahdenlaisia:

Computer Configuration - Tietokone konfiguraation käytännöt hallitsevat tietokonekohtaisia asetuksia, kuten levytilaa, tietoturvaa ja tapahtuma login hallintaa.

User configuration - Käyttäjä konfiguraation käytännöt koskevat käyttäjäkohtaisia asetuksia, kuten ohjemisto –konfigurointia, käynnistä valikon hallintaa, sekä kansion uudelleenohjausta. (Mark Minasi, Kevin Greene, Christian Booth, Robert Butler, John McCabe, Robert Panek, Michael Rice, Stefan Roth 2014, 468)

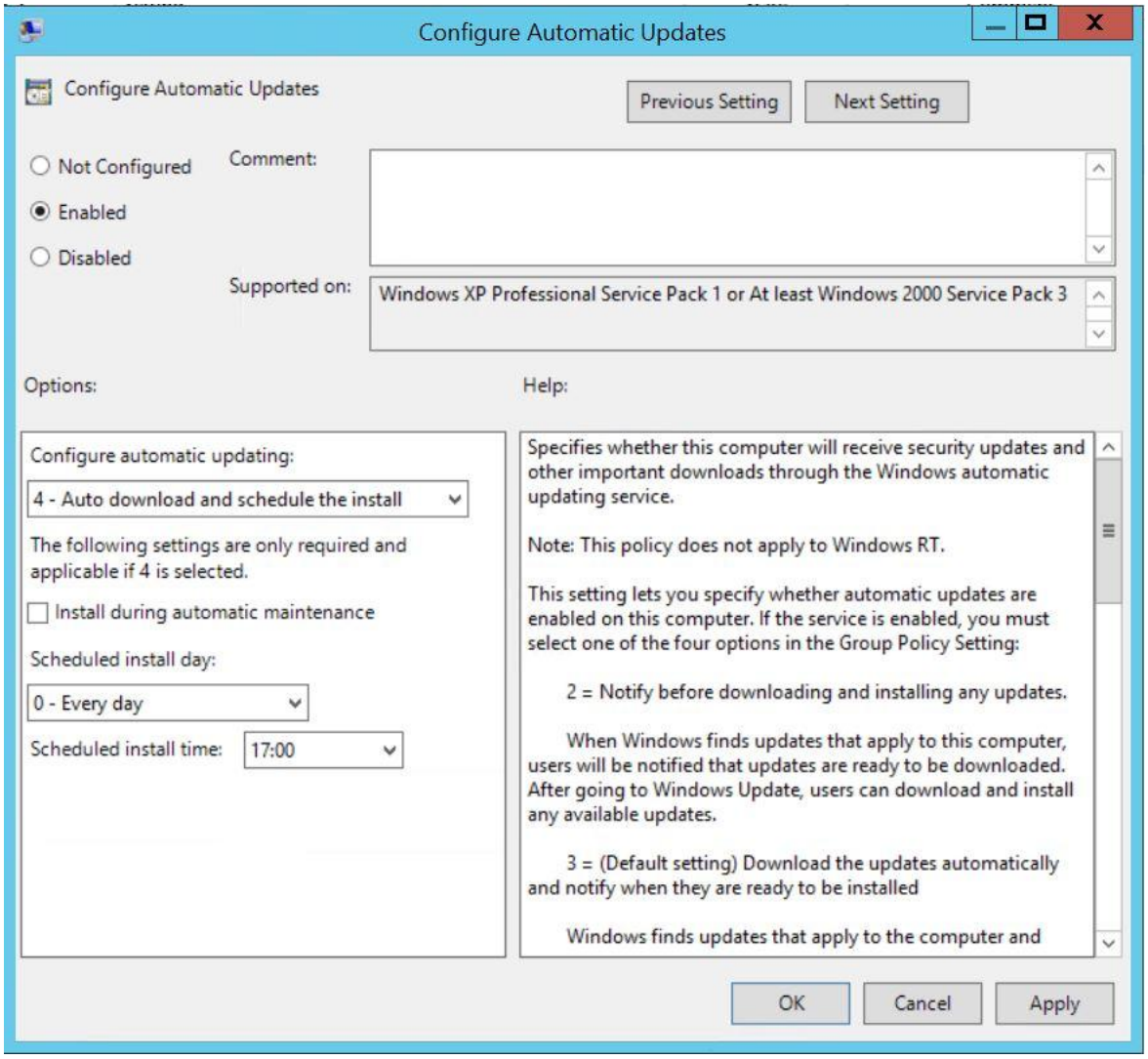
Jotta projektiympäristön työasemat saatiin näkyviin WSUS-konsolissa, luotiin työasemille oma organisaatioyksikkö ”wsus-workstations”. Työasemat siirrettiin aktiivihakemiston avulla wsus-workstations organisaatioyksikköön. Tämän jälkeen loin ryhmäkäytännön ”Enable WSUS”. Kuvassa 5. luodaan ryhmäkäytäntö ”Enable WSUS”.



Kuva 5. Ryhmäkäytäntö ”Enable WSUS”.

Ryhmäkäytäntöjen muutokset tehtiin Group Policy Management -ohjelmalla polusta: Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update.

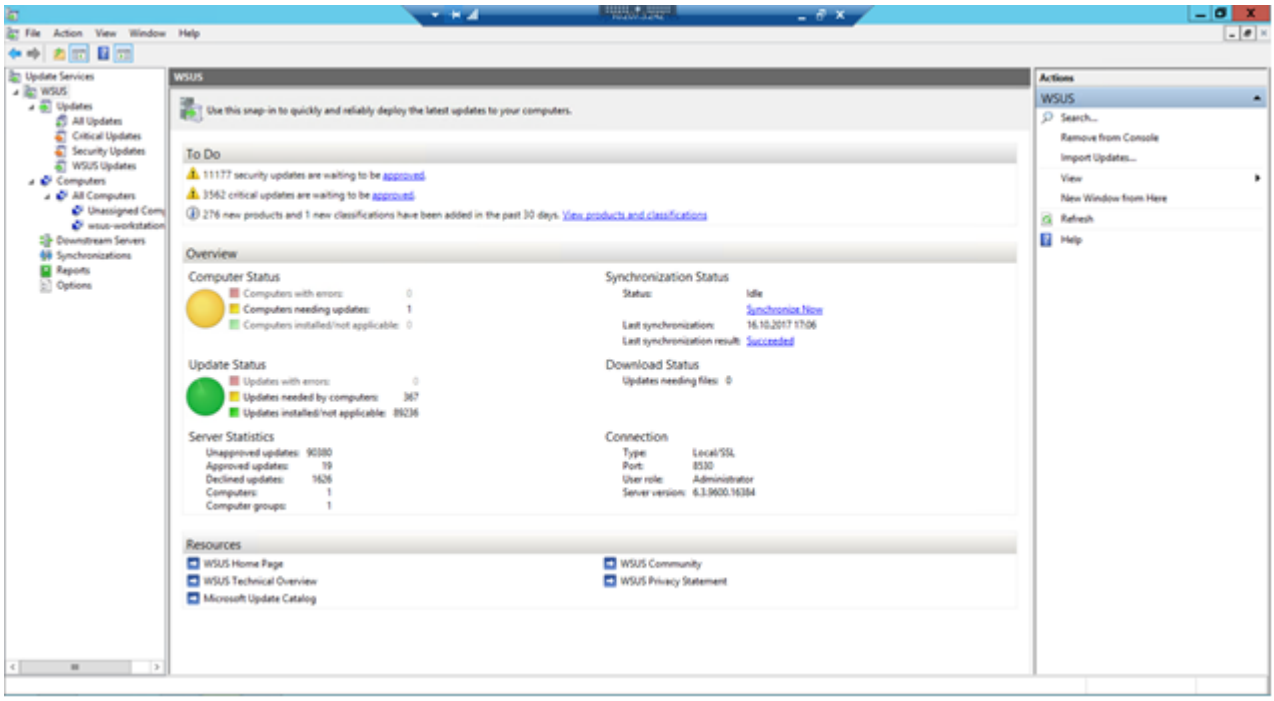
Ryhmäkäytännölle määritettiin kuinka usein Windows päivitykset ladataan ja asennetaan työasemille. Päivitykset määritettiin latautumaan automaattisesti ja päivitykset asennetaan päivittäin klo 17:00. Ryhmäkäytäntöjen avulla määritettiin myös kohderyhmä ”wsus-workstations” vastaanottamaan päivityksiä, sekä update palvelun sijainniksi palvelimen isäntänimi ja WSUSin käyttämä HTTPS -protokollan portti 8530. Lopulta ryhmäkäytännöt liitettiin organisaatioyksikköön wsus-workstations.



Kuva 6. Ryhmäkäytäntö ”Automatic updates”.

5.3 Windows päivitysten keskitetty hallinta

WSUS konsoli ilmoittaa suoraan snap-in valikossa paljonko tietoturvapäivityksä ja kriittisiä päivityksiä odottaa hyväksyntää. Valikko näyttää myös saman tien, kuinka moni työasema tarvitsee päivityksiä, jotka on hyväksytty, onko asennuksessa ilmennyt virheitä ja ovatko päivitykset asentuneet onnistuneesti. Kuvassa 7. näkyy WSUS -konsolin aloitusnäkymä.



Kuva 7. WSUS -konsoli.

Kun uusi työasema lisätään toimialueeseen ja siiretään työasema wsus-workstation organisaatioyksikön alle, ilmestyy työasema oletuksena ”Unassigned Computers” valikon alle. Työaseman ilmestymisessä WSUS -konsolin tietokoneryhmään voi mennä jonkin verran aikaa. Tätä prosessia saa kuitenkin nopeutettua avamalla työasemalta komentokehoitteen ja kirjoittamalla alla olevat komennot:

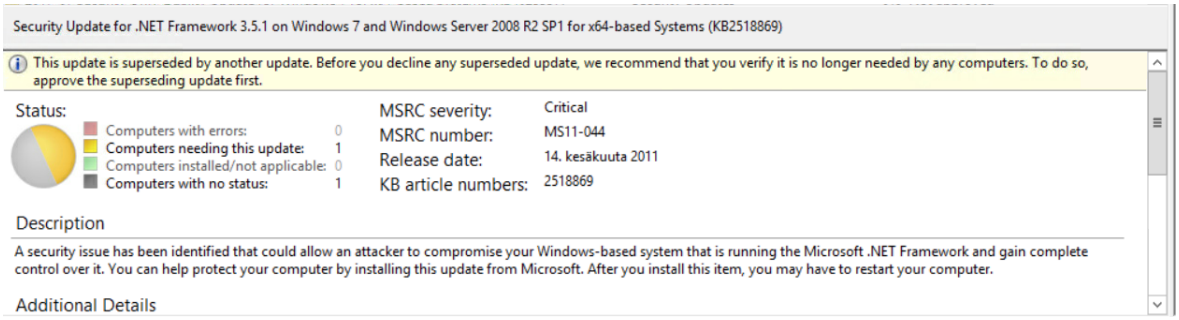
gpupdate /force
wuauclt.exe /detectnow
wuauclt.exe /reportnow

Gpupdate /force -komento pakottaa työaseman päivittämään viimeisemmät ryhmäkäytännöt.

Wuauclt.exe /detectnow ja *wuauclt.exe /reportnow* -komennot pakottavat työaseman havaitsemaan WSUS-palvelimen päivitykset ja raportoimaan tiedot palvelimelle.

Ohjasin työasemat automaattisesti oikeaan tietokoneryhmään valitsemalla WSUS-konsolissa Options > Computers > ”Use Group Policy or registry settings on computer”. Tämän jälkeen työasemat ilmestyivät automaattisesti ”wsus-workstations” tietokoneryhmään.

Kun Windows päivityksiä ollaan hyväksymässä saattaa päivityksen kohdalla lukea: ” The update is superseded by another update. Before you decline any superseded update, we recommend that you verify it is no longer needed by any computers. To do so, approve the superseding update first.”. Tämä tarkoittaa, että päivitys on korvattu jollakin toisella päivityksellä. (TechnetB) On myös mahdollista, että päivityksessä lukee ”This update supersedes another update”, joka tarkoittaa sitä, että päivitys korvaa jonkun toisen päivityksen. Kuvassa 8. WSUS ilmoittaa, että kyseinen päivitys on korvattu uudella päivityksellä.



Kuva 8. Korvattu päivitys.

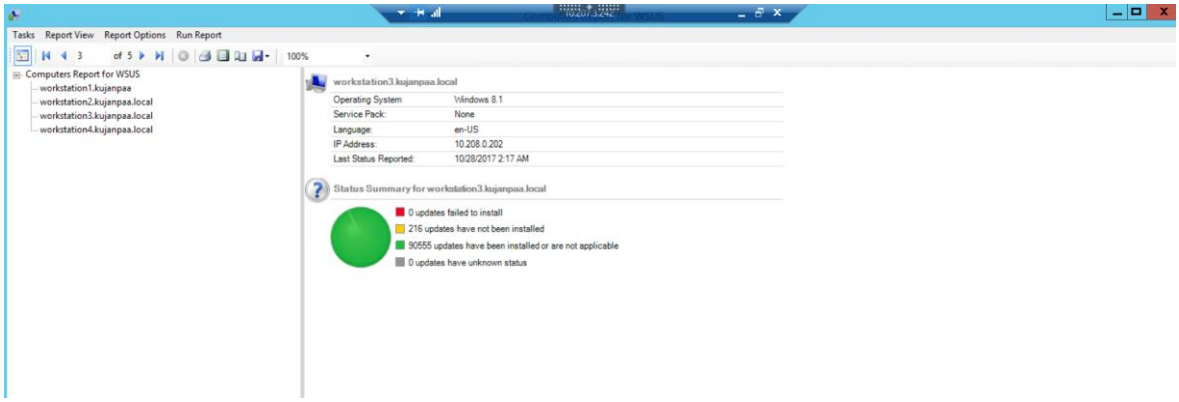
Päivitys saatetaan korvata uudella päivityksellä seuraavista syistä:
Päivitys korjaa samankaltaisen haavoittuvuuden, kuin uudempi päivitys.
Päivitys päivittää ohjelmiston aikaisemman version tai konfiguraation. (TechnetB)

5.4 Microsoft Report Viewer 2008

Jotta Windows Server Update Services -konsolin raportteihin päästiin käsiksi, tuli palvelimelle asentaa Microsoft Report Viewer 2008 -ohjelmisto. Ennen Microsoft Report Viewer 2008 raportointi työkalun asennusta palvelimelle piti asentaa .NET Framework 3.5 SP1 Add Roles and Features Wizardista. Microsoft Report Viewer antoi asentuessaan ainoastaan ilmoituksen että ”asennus suoritettiin onnistuneesti”. WSUS -konsoli täytyi käynnistää uudestaan, ennen kuin Microsoft Report Viewer asennus tuli voimaan WSUS-konsoliin ja ”Reports” valikot saatiin käyttöön. Mikäli Microsoft Report Viewer 2008 -ohjelmistoa ei ole asennettu palvelimelle, antaa ”Reports” -valikko virheilmoituksen: The Microsoft Report Viewer 2008 Redistributable is required for this feature.” Kuvassa 9. ”Reports” -valikon näkymä Microsoft Report Viewer 2008 -ohjelmiston asennuksen jälkeen.

Kuva 9. Reports -valikko.

”Reports” -valikosta löytyy kolme raportoinnin pääkategoriaa: päivitys raportit (Update Reports), tietokone raportit (Computer reports), sekä synkronointi raportit (Synchronization reports). Päivitys raporteilla saadaan tietoa esimerkiksi tiettyjen päivitysten tilasta, kuten kuinka monelle tietokoneelle päivitys on asentunut oikein ja kuinka monelle asennus ei ole onnistunut. On myös mahdollista listata, mitkä päivitykset on hyväksytty millekin WSUS -tietokoneryhmälle ja mitä päivityksiä on vielä hyväksymättä. Tietokone raporteilla saa esimerkiksi kerättyä statistiikkaa yksittäisistä tietokoneista. On mahdollista tarkastaa paljonko päivityksiä tietylle tietokoneelle, on asennettu, paljonko on asentamatta ja onko asennuksia epäonnistunut. Synkronointi raporteista näkee, kuinka paljon uusia päivityksiä on synkronoitu WSUS-palveluun Windows Update -palvelusta, kullakin synkronointi kerralla. Raportti näyttää milloin synkronointi on tehty, sekä montako päivitystä vanheni viimeisimmän synkronoinnin myötä ja montako päivitystä uusittiin viimeisimmän synkronoinnin jälkeen. Kuvasta 10. näkee, minkälaista raporttia tietokoneista saadaan WSUS –palvelun avulla.



Kuva 10. Tietokoneiden tilan -raportointi.

5.5 WSUS käyttäjän näkökulmasta

WSUS -palvelu itsessään ei juurikaan näy loppukäyttäjälle. Kun Windows päivityksiä hallitaan keskitetysti WSUS -palvelun avulla, rajaa se lähinnä loppukäyttäjän mahdollisuuksia muuttaa Windows Update -ohjelman asetuksia tietokoneella. Testityöasemalla Windows Update ”Muuta asetuksia” -välilehti antoikin ilmoituksen ”Some settings are managed by your system administrator. ” Asetukset eivät anna muokata milloin päivitykset ladataan ja asennetaan, koska ne määritettiin latautumaan ja asentumaan päivittäin klo 17:00 tietokoneelle ryhmäkäytäntöjen avulla. Päivitysten asennuksen ajankohta valittiin sillä perusteella, että niin sanottu toimistotyöaika on yleensä klo 7:00-17:00 välillä. Mikäli työasemaympäristönä olisi oikean yrityksen ympäristö, asentuisivat päivitykset niin sanotusti toimistoaikojen ulkopuolella.

6 WSUS vai Windowsin automaattiset päivitykset?

Yksittäiselle henkilölle WSUS –palvelu itsessään ei tarjoa suurta hyötyä, sillä palvelimen asentaminen ja konfigurointi ovat paljon työtä vaativa prosessi verratuna Windowsin automaattisten päivitysten käyttöön. Windowsin automaattisilla päivityksillä tietokoneen saa pidettyä ajan tasalla muutamalla hiiren klikkauksella, eikä asetuksia tarvitse määriittää erikseen kovinkaan paljoa. WSUS –palvelua varten joutuu kuitenkin luomaan toimialueen, ottamaan käyttöön Aktiivihakemiston, konfiguroimaan palomuurin, sekä tietenkin konfiguroimaan ja asentamaan WSUS –palvelun. WSUS –palvelu soveltuukin erittäin hyvin pienen ja keskisuuren yrityksen käyttöön. Mikäli tietokoneita on ylläpidettävänä alle kymmenen kappaletta, käyttäisin itse todennäköisesti Windowsin automaattiset päivitykset ominaisuutta sen helppouden vuoksi. Yli kymmenen tietokoneen ympäristöön harkitsisin WSUS –palvelun käyttöönottoa sen automatisoinnin ja valvontatyökalujen vuoksi. WSUS –palvelun avulla on mahdollista valvoa tietokoneiden päivityshistoriaa ilman kirjautumista loppukäyttäjän tietokoneelle. Tämä helpottaa yli kymmenen tietokoneen ympäristön valvontaa ja ylläpitämistä huomattavasti. Yrityksen tietokoneiden ylläpitoa ajatellen paras tilanne olisikin se, että tietty päivitys hyväksytään WSUS –konsolissa ja jaetaan vain tietyn testiryhmän tietokoneille ennen jakelua tuotantoympäristöön. Tällöin uusien Windows päivitysten toimintaa ja käyttäytymistä on mahdollista kokeilla ja tutkia yrityksen käyttämien ohjelmistojen kanssa, ennen kuin päivitykset jaetaan koko tuontatoympäristölle. Yksittäinen päivitys voi rikkoa kokonaisen sovelluksen tai kaataa sen hetkellisesti. Pahimmassa tapauksessa tämä puolestaan voi aiheuttaa koko tuotannon pysähtymisen yrityksen sisällä hetkeksi tai pidemmäksi aikaa.

7 Pohdinta

Windows Server Update Servicen avulla päivitysten asentaminen on huomattavasti hallitumpaa yrityksen tietokoneille kuin se, että päivitykset asentaisi suoraan tietokoneelle Windows Update -palvelun kautta Microsoftin -palvelimilta.
Ilman WSUS -palvelua esimerkiksi työasemalle voisi asentua hotfix, jota ei ole yrityksen sisällä vielä testattu. Ilman testiasennuksia Hotfix voi aiheuttaa työaseympäristössä ongelmia ohjelmassa jolle se on tarkoitettu. Tämä puolestaan aiheuttaa mahdollisesti ylimääräistä työtä loppukäyttäjälle tai IT-palvelun tarjoajalle, joka joutuu ongelman korjaamaan.

Mikäli päivitysten asentaminen on kokonaan jätetty loppukäyttäjien vastuulle ja Windows update -palvelu hakee päivityksiä hallitsemattomasta, on lähes mahdotonta saada selville ilman etäyhteyttä tai pääsyä loppukäyttäjän tietokoneelle, onko viimeisimmät päivitykset asennettu tietokoneelle. Tämä puolestaan voi altistaa tietokoneet useille tietoturvauhkille. WSUS -konsolin raportointityökalu on tämän vuoksi erittäin käytännöllinen työkalu työasemien valvontaa ajatellen. Mikäli yritys haluaa huolehtia tietoturvastaan, on Windows Server Update Services -palvelun tai vastaavan ohjelmiston käyttöönottaminen mielestäni erittäin suositeltavaa. Vastaavia ohjelmia joilla Windows päivityksiä pystytään jakamaan työasemiin keskitetysti, löytyy jonkin verran mm. Microsoftin System Center Configuration Manager (SCCM).

Windows server update servicen asennus ja konfigurointi on tehty suhteellisen yksinkertaiseksi ja siihen löytyi useita asennusohjeita internetistä esimerkiksi ihan suoraan Microsoftin sivuilta. Mielestäni suurin työ WSUS -palvelun käyttöönotossa on asetusten määrittäminen, kuten ryhmäkäytäntöjen luominen ja palomuurin konfigurointi.

Huomasin WSUS -konsolin latausaikojen olevan huomattavan pitkiä. Esimerkiksi päivitysten hyväksyntää varten avattavan ikkunan aukeamiseen saattoi mennä yli minuutti. Syy tähän voi tietysti olla jokin aivan muu kuin itse WSUS-palvelu. Esim. virtuaalipalvelin kuormituksella, CloudPlatformin toimivuudella ja monilla muilla tekijöillä saattaa olla vaikutusta tähän. Tuntuu hieman omituiselta, että raportointityökaluihin käsiksi pääseminen vaatii erikseen Microsoft Report Viewer 2008 -ohjelmiston asennuksen. Ohjelmiston tulisi mielestäni asentua palvelimelle WSUS-palvelun käyttöönoton yhteydessä.

Päivitysten jakaminen työasemille sujui projektin aikana hyvin, eikä yhdenkään päivityksen kanssa ollut ongelmia. Tähän tosin vaikuttaa osaltaan se, että virtuaalityöasemat ovat olleet lähestulkoon koko ajan päällä ja verkossa. Mikäli kyseessä olisi yrityksen hallinnassa olevia työasemia, voisi ongelmia päivitysten kanssa esiintyä enemmän. Mahdollisia ongelmatilanteita voisi syntyä esimerkiksi silloin kun tietokone on suljettuna, yhdistettynä langattomaan verkkoon tai käyttäjän katkaistessa virta tietokoneesta päivitysten asennuksen aikana.

Projektia olisi mahdollista jatkaa esimerkiksi asentamalla Microsoftin System Center Configuration Manager -ohjelma palvelimelle ja jakaa Windows -päivitykset sen avulla. Testiympäristöön voisi myös asentaa palvelimia joihin voisi ottaa myös WSUS-palvelun käyttöön siten, että vain yksi palvelin olisi Microsoft Update -palveluun yhdistettynä eli tomisi upstream -palvelimena. WSUS tietokanta olisi myös mahdollista määrittää toimimaan erillisellä SQL -palvelimella. Näiden toimenpiteiden hyödyt liittyvät suurilta osin palvelimen kuorman jakamiseen muille palvelimille.

Lähteet

Andrew Bettany, Mike Halsey 2017. Windows Virus and Malware Troubleshooting

Jonathan Lemonnier 2015. What is Malware? How Malware Works & How to Remove it. Luettavissa: https://www.avg.com/en/signal/what-is-malware Luettu 12.10.2017

Corey Plett, Liza Poggemeyer 2017. Windows Server Update Services (WSUS). Luettavissa: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus#wsus-server-role-description. Luettu 13.10.2017

Rafal Sosnowski 2016. Windows Update categories. Luettavissa: https://blogs.technet.microsoft.com/dubaisec/2016/01/28/windows-update-categories/. Luettu 13.10.2017

Microsoft SupportA. Service Pack and Update Center. Luettavissa: https://support.microsoft.com/en-us/help/14162/windows-service-pack-and-update-center#sptabs=win7. Luettu: 14.10.2017

Mark Minasi, Kevin Greene, Christian Booth, Robert Butler, John McCabe, Robert Panek, Michael Rice, Stefan Roth 2014. Mastering Windows Server 2012 R2

TechTarget 2015. Luettavissa: http://searchenterprisedesktop.techtarget.com/tip/What-is-a-Microsoft-hotfix. Luettu 16.10.2017

TechNetA. About the Microsoft Security Response Center. Luettavissa: https://technet.microsoft.com/en-us/security/dn528958.aspx. Luettu: 18.10.2017

Microsoft SupportB. How to keep your Windows computer up-to-date. Luettavissa: https://support.microsoft.com/en-us/help/311047/how-to-keep-your-windows-computer-up-to-date Luettu: 18.10.2017

Microsoft SupportC. Luettavissa: https://support.microsoft.com/en-us/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro.

Luettu: 18.10.2017

TechnetB. About Updates. Luettavissa: https://technet.microsoft.com/en-us/library/cc708465(v=ws.10).aspx. Luettu: 18.10.2017

Utilize Windows 2010. Luettavissa: http://www.utilizewindows.com/introduction-to-windows-server-update-services-wsus/. Luettu 29.10.2017